**SYLLABUS**

## 1. Information regarding the programme

| | |
|---|---|
| 1.1 Higher education institution | **Babeș-Bolyai University** |
| 1.2 Faculty | **Mathematics and Computer Science** |
| 1.3 Department | **Computer Science** |
| 1.4 Field of study | **Computer Science** |
| 1.5 Study cycle | **Master** |
| 1.6 Study programme / Qualification | **Cyber Security** |

## 2. Information regarding the discipline

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 2.1 Name of the discipline (en) (ro) | | | **Security Audit and Risk Management / Managementul riscurilor și auditul de securitate** | | | | |
| 2.2 Course coordinator | | | Lect. dr. Darius Bufnea | | | | |
| 2.3 Seminar coordinator | | | Lect. dr. Darius Bufnea | | | | |
| 2.4. Year of study | **1** | 2.5 Semester | **1** | 2.6. Type of evaluation | **C** | 2.7 Type of discipline | **Mandatory** |
| 2.8 Code of the discipline | | **MME8191** | | | | | |

## 3. Total estimated time (hours/semester of didactic activities)

| | | | | | |
|---|---|---|---|---|---|
| 3.1 Hours per week | 4 | Of which: 3.2 course | 2 | 3.3 seminar/laboratory | 1 sem + 1pr. |
| 3.4 Total hours in the curriculum | 56 | Of which: 3.5 course | 28 | 3.6 seminar/laboratory | 28 |
| Time allotment: | | | | | hours |
| Learning using manual, course support, bibliography, course notes | | | | | 22 |
| Additional documentation (in libraries, on electronic platforms, field documentation) | | | | | 22 |
| Preparation for seminars/labs, homework, papers, portfolios and essays | | | | | 35 |
| Tutorship | | | | | 5 |
| Evaluations | | | | | 10 |
| Other activities: ..... | | | | | |

| | |
|---|---|
| 3.7 Total individual study hours | 94 |
| 3.8 Total hours per semester | 150 |
| 3.9 Number of ECTS credits | 6 |

## 4. Prerequisites (if necessary)

| | |
|---|---|
| 4.1. curriculum | • Now |
| 4.2. competencies | • Now |

**5. Conditions** (if necessary)

| | |
|---|---|
| 5.1. for the course | • Now |
| 5.2. for the seminar /lab activities | • Now |

**6. Specific competencies acquired**

| | |
|---|---|
| **Professional competencies** | • Know and understand the main paradigms related to data protection: confidentiality, integrity and data availability;<br>• Knowledge of all security aspects that can impact the processes and IT&C assets of an organization;<br>• Acquiring a solid theoretical foundation in communication through unsafe medium, as well as the use of secure communication protocols on the Internet; |
| **Transversal competencies** | • Professional communication skills; concise and precise description, both oral and written, of professional results;<br>• Ethic and fair behaviour, commitment to professional deontology;<br>• Applying the norms of organized and efficient work, responsibility and reliability of the work performed both individually and within a team;<br>• Entrepreneurial skills; working with economical knowledge; continuous learning;<br>• Good English communication skills. |

**7. Objectives of the discipline** (outcome of the acquired competencies)

| | |
|---|---|
| 7.1 General objective of the discipline | • Understanding the fundamental aspects of organization, human resources and management in the field of organization security;<br>• Understanding the activities that must be undertaken to ensure business security;<br>• Get familiar with good practices and errors that may occur in the risk management activity<br>• Get familiar with security audit methodologies |
| 7.2 Specific objective of the discipline | The promotion of the discipline must allow the master student to:<br>• Know and present which are the sections of organizational security;<br>• Be able to establish measures need to ensure the physical security;<br>• Understand and apply the methods need to ensure the information security<br>• Be able to identify vulnerabilities and security threats to an organization and business;<br>• Be able to assess the security risk using at least one of the established methods;<br>• Understand the security challenges generated by staff;<br>• Can carry out a Staff Security Training Plan;<br>• Be able to establish appropriate security treatments for each identified security risk;<br>• Be able to elaborate a security procedure;<br>• Be able to establish the steps of security audit. |

**8. Content**

| 8.1 Course | Teaching methods | Remarks |
|---|---|---|
| 1. Theoretical aspects of security. Security of organizations and businesses from necessity to legal enforcement | Lecture, explanation | |
| 2. Physical security - a central pillar in order to ensure the security of the organization | Lecture, explanation | |
| 3. Security of personnel from security risk to competitiveness. The security check of personnel | Lecture, explanation | |
| 4. Asset information is essential for any type of organization and business. From information theory to information security | Lecture, explanation | |
| 5. Implementation of information and document security systems (INFOSEC, COMSEC, etc.) | Lecture, explanation | |
| 6. Other sectors of organizational security: occupational health and safety, fire prevention and extinguishing, protection of personal data, environmental protection, etc. | Lecture, explanation | |
| 7. Identifying security risks - from theory to practice | Lecture, explanation | |
| 8. Security risk assessment techniques and methods | Lecture, explanation | |
| 9. Security risk management: strategy, monitoring, review. | Lecture, explanation | |
| 10. Implementation of risk management systems | Lecture, explanation | |
| 11. Risk management - quality management - organizational and entrepreneurial competitiveness | Lecture, explanation | |
| 12. Theoretical and practical aspects of security audit | Lecture, explanation | |
| 13. The audit process of a security management system | Lecture, explanation | |
| 14. Specific occupations in the field of organizational and business security | Lecture, explanation | |

Bibliography

*Risk Assessment and Mapping Guidelines,* Commission Staff Working Paper, European Commission, SEC(2010) 1626 final, Brussels, 2010

*Convergent Security Risks in Physical Security Systems and IT Infrastructures*, The Alliance for Enterprise Security Risk Management, Virginia 2010

*General Security Risk Assessment*, ASIS International Guideline, Alexandria, Virginia 2003

*Business Continuity Guideline: A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery*, ASIS International, 2005

*BUSINESS CONTINUITY MANAGEMENT GUIDELINES*, Second Edition, WESTERN AUSTRALIAN GOVERNMENT, July 2009

*METODOLOGIE DE MANAGEMENT AL RISCURILOR*, Secretariatul General al Guvernului României, 2018, *Programul Operațional Capacitate Administrativă cofinanțat de Uniunea Europeană, din Fondul Social European*

BRODER, James F., *Risk Analysis and the Security Survey,* THIRD EDITION, Elsevier's Science & Technology Rights Department in Oxford, UK, 2006

DEMPSEY, John S. *Introduction to Private Security,* Second Edition, Wadsworth, Cengage Learning, 2011
HESS, Karen M., *Introduction to Private Security*, Fifth Edition, Wadsworth, Cengage Learning, 2009

LANDOLL, Douglas J., *THE SECURITY RISK ASSESSMENT HANDBOOK A Complete Guide for Performing Security Risk Assessments,* Auerbach Publications Taylor & Francis Group, Boca Raton, FL 2006

NORMAN, Thomas L., *Risk Analysis and Security Countermeasure Selection*, CRC Press, Taylor and Francis Group, Boca Raton, London, New York, 2010

| 8.2 Seminar / laboratory | Teaching methods | Remarks |
|---|---|---|
| 1. Case study: Interpretation of any type of organizational and entrepreneurial activity from the perspective of ensuring security. | Debate, case study | |
| 2. Debate: The relationship between physical security and the physical security of computer systems | Debate | |
| 3. Case study: Wikileaks, Panama Papers, Edward Snowden | Debate | |
| 4. Establishing information needs in an organization. Identifying business information needs.<br>Exercise 1: Make a list of information needs for an organization or business | Debate, case study, templates presentation | Teaching exercise at the next scheduled meeting. It is a mandatory topic in the individual portfolio. |
| 5. Case study: vulnerabilities, risks and threats to information and to document security.<br>Exercise 2: Make a list of vulnerabilities, risks, and security threats to an organization or business | Debate, case study, templates presentation | Teaching exercise at the next scheduled meeting. It is a mandatory topic in the individual portfolio. |
| 6. Debate: Ensuring the health and safety of a computer scientist at work | Debate | |
| 7.Identifying the security risks of computer systems<br>Exercise 3: Make a list of the security risks of an organization or business | Debate, case study, templates presentation | Teaching exercise at the next scheduled meeting. It is a mandatory topic in the individual portfolio. |
| 8. Delphi method of risk assessment | templates presentation | |
| 9. Security risk management.<br>Exercise 4: Establishing security treatments for identified security risks (continued Exercises 2 and 3) | Explanation, debate and templates presentation | Teaching exercise at the next scheduled meeting. It is a compulsory subject. Teamwork (2-3 masters) |
| 10. Elaborating a security policy of the organization<br>Exercise 5: Develop a Security Training Plan | Explanation, debate and templates presentation | Teaching exercise at the next scheduled meeting. It is a compulsory subject. Teamwork (2-3 masters) |

| | | |
|---|---|---|
| 11. Writing a security procedure<br>Exercise 6: Perform a security procedure - optional. | Explanation, debate and templates presentation | Teaching exercise at the next scheduled meeting.<br>It is a compulsory subject.<br>Teamwork (2-3 masters) |
| 12. Debate: External audit vs. internal audit | Debate | |
| 13. The audit documentation, from planning to audit report | Explanation, debate and templates presentation | |
| 14. Cyber Security internal or outsourcing department? | Debate | |

Bibliography

*Risk Assessment and Mapping Guidelines,* Commission Staff Working Paper, European Commission, SEC(2010) 1626 final, Brussels, 2010

*Convergent Security Risks in Physical Security Systems and IT Infrastructures*, The Alliance for Enterprise Security Risk Management, Virginia 2010

*General Security Risk Assessment*, ASIS International Guideline, Alexandria, Virginia 2003

*Business Continuity Guideline: A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery*, ASIS International, 2005

*BUSINESS CONTINUITY MANAGEMENT GUIDELINES*, Second Edition, WESTERN AUSTRALIAN GOVERNMENT, July 2009

*METODOLOGIE DE MANAGEMENT AL RISCURILOR*, Secretariatul General al Guvernului României, 2018, *Programul Operațional Capacitate Administrativă cofinanțat de Uniunea Europeană, din Fondul Social European*

BRODER, James F., *Risk Analysis and the Security Survey,* THIRD EDITION, Elsevier's Science & Technology Rights Department in Oxford, UK, 2006

DEMPSEY, John S. *Introduction to Private Security,* Second Edition, Wadsworth, Cengage Learning, 2011

HESS, Karen M., *Introduction to Private Security*, Fifth Edition, Wadsworth, Cengage Learning, 2009

LANDOLL, Douglas J., *THE SECURITY RISK ASSESSMENT HANDBOOK A Complete Guide for Performing Security Risk Assessments,* Auerbach Publications Taylor & Francis Group, Boca Raton, FL 2006

NORMAN, Thomas L., *Risk Analysis and Security Countermeasure Selection*, CRC Press, Taylor and Francis Group, Boca Raton, London, New York, 2010

Fișe, modele de documente care vor fi oferite în cadrul seminarului

**9. Corroborating the content of the discipline with the expectations of the epistemic community, professional associations and representative employers within the field of the program**

• The discipline was developed in accordance with the papers in the field, published in the country and abroad;

| |
|---|
| • Some topics in the discipline include relevant issues, which are the subject of concerns of relevant institutions or national and international scientific conferences, including debates in national and international journals;<br>• The thematic content is closely related to the practical activities carried out within the organizations of private security specialists. |

**10. Evaluation**

| Type of activity | 10.1 Evaluation criteria | 10.2 Evaluation methods | 10.3 Share in the grade (%) |
|---|---|---|---|
| 10.4 Course | 1. logical coherence, fluency, expressiveness, strength of argument;<br>2. the ability to operate with the assimilated knowledge in complex intellectual activities, in conditions of stress and reduced time;<br>3. the ability to apply the learned knowledge in practice;<br>4. capacity for analysis, personal interpretation, originality, creativity;<br>5. the degree of assimilation of the specialized language and the communication capacity. | Oral support of a risk assessment (Delphi method). The master's student will also answer questions related to the theoretical content of the discipline in relation to the evaluation prepared. | 45% |
| 10.5 Seminar/lab activities | 1. the ability to operate with the knowledge assimilated in complex intellectual activities in conditions of stress and reduced time;<br>2. the ability to apply the learned knowledge in practice;<br>3. capacity for analysis, personal interpretation, originality, creativity; | Preparation of an individual portfolio consisting of:<br>Exercises 1, 2 and 3<br>- written paper and oral support in seminars<br>- is taught at the last seminar in revised form after the feedback received | 25% |
| | 1. the ability to work in a team<br>2. the ability to operate with the knowledge assimilated in complex intellectual activities, in conditions of stress and reduced time;<br>3. the ability to apply the learned knowledge in practice. | Preparation of a team portfolio consisting of:<br>Exercises 4,5 and 6<br>- written writing and oral support in seminars<br>- is taught at the last seminar in revised form after the feedback received | 20% |
| 10.6 Minimum performance standards | | | |

- writing and presenting the papers in the portfolio
- elaborating and presenting the risk assessment on a required topic
- the documents and the answers to the questions should not contain serious mistakes that would demonstrate the superficial knowledge of the content of the discipline

| Date | Signature of course coordinator | Signature of seminar coordinator |
|---|---|---|
| **28.05.2022** | **Lect. dr. Darius Bufnea** | **Lect. dr. Darius Bufnea** |

| Date of approval | Signature of the head of department |
|---|---|
| ..... | **Prof. dr. Laura Dioșan** |